Bound entanglement useful for reducing communication complexity

M Epping[1] and Č Brukner[2,3]

[1] Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstr. 1, D-40225 Düsseldorf, Germany

[2] Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria

[3] Institute of Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria

E-mail: `epping@thphy.uni-duesseldorf.de`

PACS numbers: 03.67.Hk, 03.65.Ud, 03.67.Mn

Abstract. We present a simple communication complexity problem where three parties benefit from sharing bound entanglement. This clarifies the fact that entanglement distillability of the shared state is not necessary in order to surpass classical information processing.

1. Introduction

Quantum Information studies communication or computation schemes which allow more efficient solutions when considering the laws of quantum theory instead of those of classical physics. In this research, entanglement has proven to be beneficial and many applications make use of maximally entangled states [1]. As these states are important for such applications, methods have been developed to create one maximally entangled state out of several copies of less entangled states using local operations and classical communication (LOCC) [2]. This process is called entanglement distillation. Entangled states that allow for the creation of a maximally entangled state by LOCC in at least one bipartition of the composite system are called distillable. States which are entangled but not distillable are called bound entangled [3].

Bell inequalities are constraints on probabilities for local measurements, which are satisfied by local hidden variable theories [4, 5]. However, they are not satisfied by quantum mechanics. Entangled states that violate a Bell inequality are called nonlocal. Every distillable state may be transformed into a nonlocal state using only LOCC, but not every nonlocal state is distillable. This was found recently by giving an example of a nonlocal bound entangled state [6]. Given that one cannot extract pure entanglement from bound entangled states, one may wonder if they are of any use for quantum information purposes. Here we show that bound entanglement can actually be of use in a quantum communication complexity task. Communication Complexity studies the amount of information that must be communicated between distant parties in order to calculate a function whose arguments are distributed among the parties [7]. We consider a similar question: If the parties are restricted to communicate only a given amount of information, what is the highest possible probability for them to estimate the value of the function correctly?

2. A general quantum communication complexity scheme

We will make use of a generalization of the quantum communication complexity scheme introduced in Ref. [8] to more than two bits input per party. Consider the situtation where n parties labelled 1 to n are spatially separated. Let us assume a Bell inequality of the form

$$\sum_{x_1,...,x_n=0}^{2^m-1} g(x_1,...,x_n)E(x_1,...,x_n) \leq B, \tag{1}$$

where the coefficients $g(x_1,...,x_n)$ and the local hidden variable bound B are real numbers and $E(x_1,...,x_n)$ is the correlation function of a measurement for the choice of measurement setting x_i by each party i. The correlation function can be expressed as $E(x_1,...,x_n) = P(a_1...a_n = 1|x_1,...,x_n) - P(a_1...a_n = -1|x_1...x_n)$, where $a_i = \pm 1$ is the measurement result of observer i. In quantum mechanics, the Bell inequality can be violated by a value $S > B$. Following the idea of Ref. [8] we introduce a quantum communication complexity problem associated with this Bell inequality. Each party i

receives one bit $y_i \in \{-1, 1\}$ and m bits $x_i \in \{0, 1, ..., 2^m - 1\}$ unknown to all the other parties. The two possible values of y_i occur with equal probability while the values of x_i follow the probability distribution

$$Q(x_1, ..., x_n) = \frac{|g(x_1, ..., x_n)|}{\sum_{x'_1,...,x'_n=0}^{2^m-1} |g(x'_1, ..., x'_n)|}. \quad (2)$$

The common task of all parties is to output the value of the function

$$f(y_1, ..., y_n, x_1, ..., x_n) = \prod_{i=1}^{n} y_i \text{sign}\left[g(x_1, ..., x_n)\right]. \quad (3)$$

The parties will not evaluate the function correctly with certainty. The aim is to maximize the probability of successful evaluation. Each party is allowed to broadcast a single bit of information to its fellow parties. It is required that all parties broadcast the bit simultaneously (in this way the communicated bit of one party does not depend on the broadcasted bits of others, but only on the local input). Afterwards one of the parties is asked to output the value of the function. We consider two different protocols. In the classical protocol the bit s_i sent by party i is a function of y_i and x_i. It was shown in Ref. [9] (analog to Ref. [8]) that in the optimal classical protocol $s_i = y_i a_i(x_i)$ where $a_i(x_i)$ is an appropriate chosen function $\{0, 1, ..., 2^m - 1\} \to \{-1, 1\}$ and the best guess is given by

$$A(y_1, ..., y_n, x_1, ..., x_n) = \prod_{i=1}^{n} y_i a_i(x_i). \quad (4)$$

In the quantum protocol $a_i(x_i)$ is replaced by the measurement result a_i. Each party i chooses one out of 2^m possible measurement settings according to the input x_i and sends y_i multiplied by the measurement result a_i. The best guess is then again given by Eq. 4.

The probability of success of the protocol, i.e. the probability for $A(y_1, ..., y_n, x_1, ..., x_n)$ to equal $f(y_1, ..., y_n, x_1, ..., x_n)$ can be written as

$$P(A = f) = \frac{1}{2}\left[1 + (f, A)\right] \quad (5)$$

using the weighted scalar product

$$(f, A) = \sum_{y_1,...,y_n=\pm 1} \sum_{x_1,...,x_n=0}^{2^m-1} \frac{1}{2^n} Q(x_1, ..., x_n) f(y_1, ..., x_n) A(y_1, ..., x_n). \quad (6)$$

Inserting Q, f and A gives the probability of guessing correctly

$$P_C = \frac{1}{2}\left(1 + \frac{B}{\sum_{x_1,...,x_n=0}^{2^m-1} |g(x_1, ..., x_n)|}\right) \quad (7)$$

in the classical protocol and

$$P_Q = \frac{1}{2}\left(1 + \frac{S}{\sum_{x_1,...,x_n=0}^{2^m-1} |g(x_1, ..., x_n)|}\right) \quad (8)$$

in the quantum case.

3. Bound entanglement as a resource

We now come to the explicit example. We choose $n = 3$, so there are three separated parties. They share the state

$$\rho = \sum_{i=1}^{4} p_i |\psi_i\rangle\langle\psi_i| \tag{9}$$

with $p_1 = 0.0636039$, $p_2 = p_3 = 0.273734$, $p_4 = 0.388929$ and

$$|\psi_1\rangle = 0.183013|000\rangle - 0.408248\,(|001\rangle + |010\rangle + |100\rangle) + 0.683013|111\rangle,$$
$$|\psi_2\rangle = -0.344106(|001\rangle - 2|010\rangle + |100\rangle) + 0.219677(|011\rangle - 2|101\rangle + |110\rangle),$$
$$|\psi_3\rangle = 0.596008(|100\rangle - |001\rangle) + 0.380492(|110\rangle - |011\rangle),$$
$$|\psi_4\rangle = -0.933013|000\rangle + 0.149429(|011\rangle + |101\rangle + |110\rangle) + 0.25|111\rangle.$$

It was introduced by T. Vértesi and N. Brunner in Ref. [6]. See the reference for an analytic expression for the amplitudes. It is constructed such that it is symmetric under permutations of the parties and invariant under partial transpose with respect to party 3. The last condition is sufficient for ρ to be biseparable on the partition $(1,2)|3$ [10]. Together these conditions ensure that the state is separable along any biseparation. Therefore it is fully nondistillable. Here "fully nondistillable" refers to the fact that none of the three groupings $(1,2)|3$, $(1,3)|2$ and $(2,3)|1$ of subsystems to parties is distillable. Vértesi and Brunner also found that ρ can be used to violate the Bell inequality

$$-13 \leq \mathrm{sym}[A_1 + A_1B_2 - A_2B_2 - A_1B_1C_1 - A_2B_1C_1 + A_2B_2C_2] \leq 3, \tag{10}$$

which is listed under number 5 in Ref. [11]. The symbol $\mathrm{sym}[X]$ denotes the symmetrization of X with respect to the three parties, e.g. $\mathrm{sym}[A_1B_2] = A_1B_2 + A_1C_2 + A_2B_1 + A_2C_1 + B_1C_2 + B_2C_1$. As ρ is fully nondistillable and nonlocal it is fully bound entangled.

We now use the method of homogenization described by Y. Wu and M. Żukowski in Ref. [12]: By adding a constant 5 to inequality (10) the bounds become symmetric. Then we introduce new observables A_0, B_0 and C_0 which also take the values -1 and 1. Substituting the observables A_i by A_i/A_0, B_i by B_i/B_0 and C_i by C_i/C_0 and factoring out $1/(A_0B_0C_0)$, one expands lower order correlation terms to full correlation terms. We arrive at the inequality

$$\begin{aligned} &\left|\frac{1}{A_0B_0C_0}\mathrm{sym}[\,5A_0B_0C_0 + A_1B_0C_0 + A_1B_2C_0 - A_2B_2C_0 \right.\\ &\qquad\qquad \left. - A_1B_1C_1 - A_2B_1C_1 + A_2B_2C_2]\right| \leq 8 \\ \Leftrightarrow\quad &|\mathrm{sym}[5A_0B_0C_0 + A_1B_0C_0 + A_1B_2C_0 - A_2B_2C_0 \\ &\qquad\qquad - A_1B_1C_1 - A_2B_1C_1 + A_2B_2C_2]| \leq 8, \end{aligned} \tag{11}$$

which is expression H05 given in table I of Ref. [12]. This inequality has the required form to link to the communication complexity problem described above. Like in Ref. [6] we choose

$$A_1 = B_1 = C_1 = \begin{pmatrix} \cos\left(\frac{2\pi}{9}\right) & \sin\left(\frac{2\pi}{9}\right) \\ \sin\left(\frac{2\pi}{9}\right) & -\cos\left(\frac{2\pi}{9}\right) \end{pmatrix} \tag{12}$$

$$\text{and } A_2 = B_2 = C_2 = \begin{pmatrix} \sin\left(\frac{\pi}{18}\right) & -\cos\left(\frac{\pi}{18}\right) \\ -\cos\left(\frac{\pi}{18}\right) & -\sin\left(\frac{\pi}{18}\right) \end{pmatrix}. \tag{13}$$

For the new observables it is sufficient to choose $A_0 = B_0 = C_0 = \mathbb{1}$. With these observables we calculate the left-hand side of (11) using the quantum mechanical expectation values as

$$S = 5 + 3.00685 = 8.00685. \tag{14}$$

This violation of the Bell inequality (11) implies a quantum advantage in the quantum communication complexity task associated with it. We write the coefficients in front of correlations $A_{x_1}B_{x_2}C_{x_3}$ in inequality (11) as

$$\begin{aligned} g(x_1, x_2, x_3) = &\ \{2\left[(\delta_{x_1,x_2,x_3} + x_1 + x_2 + x_3) \bmod 2\right] - 1\} \\ &\times (1 + 4\delta_{0,x_1,x_2,x_3})(1 - \delta_{2,(x_1+x_2+x_3) \bmod 3}) \prod_{i=1}^{3} (1 - \delta_{3,x_i}), \end{aligned} \tag{15}$$

where the symbol δ is 1 if all subscripts are equal and 0 otherwise. The first factor of Eq. 15 gives the sign of the coefficient while the others define the probability distribution for x_1, x_2 and x_3 (see Eq. 2). The task for the three parties is to calculate the function

$$\begin{aligned} f &= y_1 y_2 y_3 \mathrm{sign}\left[g(x_1, x_2, x_3)\right] \\ &= y_1 y_2 y_3 \left\{2\left[(\delta_{x_1,x_2,x_3} + x_1 + x_2 + x_3) \bmod 2\right] - 1\right\}. \end{aligned} \tag{16}$$

As we chose $A_0 = B_0 = C_0 = \mathbb{1}$ a party i performs no measurement if $x_i = 0$ and simply sends y_i. Using equations (7) and (8) we get $P_C = 0.681818$ and $P_Q = 0.681974$. This shows that the parties can increase the probability of success if they share the bound entangled state ρ, as compared to any classical protocol. Therefore it is a simple application associated with the Bell inequality (10) the authors of Ref. [6] were asking for. We note that a similar advantage can be shown using the nonlocal games from Ref. [13].

Acknowledgments

We thank Sylvia Bratzik and Dagmar Bruß for advising us to this topic. ME is supported by Deutsche Forschungsgemeinschaft (DFG). CB acknowledges support from the European Commission, Q-ESSENCE (No 248095) and the Austrian Science Fund (FWF): [SFB-FOCUS], [P 24621] and the doctoral programme CoQuS.

References

[1] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information.* Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2000.

[2] Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and William K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 76:722–725, Jan 1996.

[3] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature? *Phys. Rev. Lett.*, 80:5239–5242, Jun 1998.

[4] John Stewart Bell. On the einstein podolski rosen paradox. *Physics*, 1:195–200, 1964.

[5] Asher Peres. All the bell inequalities. *Foundations of Physics*, 29:589–614, 1999.

[6] Tamás Vértesi and Nicolas Brunner. Quantum nonlocality does not imply entanglement distillability. *Phys. Rev. Lett.*, 108:030403, Jan 2012.

[7] Eyal Kushilevitz and Noam Nisan. *Communication complexity.* Cambridge University Press, New York, NY, USA, 1997.

[8] Caslav Brukner, Marek Żukowski, Jian-Wei Pan, and Anton Zeilinger. Bell's inequalities and quantum communication complexity. *Phys. Rev. Lett.*, 92:127901, Mar 2004.

[9] Michael Epping. Quantenkommunikationskomplexität mit nichtidealen detektoren. Master's thesis, University of Vienna, Austria, 2012.

[10] B. Kraus, J. I. Cirac, S. Karnas, and M. Lewenstein. Separability in $2 \times n$ composite quantum systems. *Phys. Rev. A*, 61:062302, May 2000.

[11] Cezary Sliwa. Symmetries of the bell correlation inequalities. *Physics Letters A*, 317(3 - 4):165 – 168, 2003.

[12] Yu-Chun Wu and Marek Żukowski. Homogenization of bell inequalities. *Phys. Rev. A*, 85:022119, Feb 2012.

[13] J. Silman, S. Machnes, and N. Aharon. On the relation between bell's inequalities and nonlocal games. *Physics Letters A*, 372(21):3796 – 3800, 2008.